to obtain the MGF of the instantaneous SNR at the combiner output. Based on this result and applying the MGF-based method, the average SEP has then been attained in terms of the distinct eigenvalues of the Gaussian components and their associated algebraic multiplicities. The approach has been applied to some special cases, such as the dual-branch correlated and the independent multichannel case, and agreements with previously reported results have been verified. Furthermore, although the analysis focused on rectangular QAM constellations, the proposed approach can easily be extended to other M-ary modulation schemes.

REFERENCES

[1] G. D. Durgin, T. S. Rappaport, and D. A. de Wolf, "New analytical models and probability density functions for fading in wireless communications," *IEEE Trans. Commun.*, vol. 50, no. 6, pp. 1005–1015, Jun. 2002.

[2] M. D. Yacoub, "The κ–μ distribution and the η–μ distribution," *IEEE Antennas Propag. Mag.*, vol. 49, no. 1, pp. 68–81, Feb. 2007.

[3] M. K. Simon and M.-S. Alouini, *Digital Communication Over Fading Channels,* 2nd ed. Hoboken, NJ: Wiley, 2005.

[4] N. Beaulieu, "A useful integral for wireless communication theory and its application to rectangular signaling constellation error rates," *IEEE Trans. Commun.*, vol. 54, no. 5, pp. 802–805, May 2006.

[5] A. Maaref and S. Aïssa, "Exact error probability analysis of rectangular QAM for single- and multichannel reception in Nakagami-m fading channels," *IEEE Trans. Commun.*, vol. 57, no. 1, pp. 214–221, Jan. 2008.

[6] N. Y. Ermolova, "Useful integrals for performance evaluation of communication systems in generalised η–μ and κ–μ fading channels," *IET Commun.*, vol. 3, no. 2, pp. 303–308, Feb. 2009.

[7] D. B. da Costa and M. D. Yacoub, "Accurate approximations to the sum of generalized random variables and applications in the performance analysis of diversity systems," *IEEE Trans. Commun.*, vol. 57, no. 5, pp. 1271–1274, May 2009.

[8] P. R. Krishnaiah and M. M. Rao, "Remarks on a multivariate gamma distribution," *Amer. Math. Mon.*, vol. 68, no. 4, pp. 342–346, Apr. 1961.

[9] H. Exton, *Multiple Hypergeometric Functions and Applications*. New York: Wiley, 1976.

[10] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables,* 9th ed. New York: Dover, 1970.

[11] M.-S. Alouini, A. Abdi, and M. Kaveh, "Sum of gamma variates and performance of wireless communication systems over Nakagami-fading channels," *IEEE Trans. Veh. Technol.*, vol. 50, no. 6, pp. 1471–1480, Nov. 2001.

[12] M. Z. Win, G. Chrisikos, and J. H. Winters, "MRC performance for M-ary modulation in arbitrarily correlated Nakagami fading channels," *IEEE Commun. Lett.*, vol. 4, no. 10, pp. 301–303, Oct. 2000.

[13] M. V. Clark, L. J. Greenstein, W. K. Kennedy, and M. Shafi, "Matched filter performance bounds for diversity combining receivers in digital mobile radio," *IEEE Trans. Veh. Technol.*, vol. 41, no. 4, pp. 356–362, Nov. 1992.

[14] H. Vincent Poor, *An Introduction to Signal Detection and Estimation,* 2nd ed. New York: Springer-Verlag, 1994.

[15] A. Papoulis, *Probability, Random Variables, and Stochastic Processes,* 4th ed. New York: McGraw-Hill, 2002.

Comments on "Proving Reliability of Anonymous Information in VANETs" by Kounga *et al.*

Liqun Chen, *Member, IEEE*, and Siaw-Lynn Ng

***Abstract*—Three vehicle-to-vehicle communication schemes by Kounga *et al.* ("Proving reliability of anonymous information in VANETs," *IEEE Trans. Veh. Technol.*, vol. 58, no. 6, pp. 2977–2989, Jul. 2009) were recently published to address the issues of certificate management, scalability, and privacy. We present a number of attacks on one of the schemes. Our result shows that, contrary to what is claimed, this scheme does not provide the following four security features: 1) authenticity of a message; 2) privacy of drivers and vehicles; 3) reliability of distributed information; and 4) revocation of illegitimate vehicles.**

***Index Terms*—Anonymity, authentication, vehicular communication.**

I. INTRODUCTION

In a vehicular ad hoc network, vehicle-to-vehicle communications allow vehicles to exchange information about road or traffic conditions, thereby enabling a safer and more conducive travelling environment. Security requirements for such communications have been studied by various authors and organizations, and we refer to [4] and [6] for extensive overviews and references.

For the purpose of this paper, we first briefly review the following four concerns in this context: 1) the authenticity of a message; 2) the privacy of the drivers and vehicles; 3) the reliability of distributed information; and 4) the revocation of illegitimate vehicles.

On the question of the authenticity of a message, one solution is to ensure that a message originated from a legitimate source. In the literature of vehicle-to-vehicle communications, this property is achieved by using a cryptographic data chain, starting with a trusted third party (TTP) and ending up with a message announcement. The TTP distributes credentials to legitimate vehicles. One example of such a TTP is a certification authority (CA), and the distributed credentials are public key certificates (e.g., [4] and [6]). These vehicles use the certified public keys to either sign an announcement or introduce further credentials as part of the data chain. It guarantees that the announced message has been created by a legitimate vehicle and that the validity of the data chain is publicly verifiable.

In general, user privacy[1] includes two aspects, namely, anonymity and unlinkability. Anonymity of drivers and vehicles can be protected by using pseudonyms that do not indicate their owners' identities. Unlinkability means that different messages sent by a vehicle should not be identified as coming from one source. This property prevents user tracking and profiling, and as shown in the literature, it can be achieved by using different pseudonyms for different announcements (e.g., [1] and [4]–[6]).

Manuscript received June 30, 2009; revised October 20, 2009. First published December 18, 2009; current version published March 19, 2010. The review of this paper was coordinated by Dr. L. Cai.

L. Chen is with Hewlett-Packard Labs, Bristol, BS34 8QZ U.K. (e-mail: liqun.chen@hp.com).

S.-L. Ng is with the Information Security Group, Mathematics Department, Royal Holloway, University of London, Surrey TW20 0EX, U.K. (e-mail: s.ng@rhul.ac.uk).

Digital Object Identifier 10.1109/TVT.2009.2038785

[1]There are a number of different interpretations of user privacy. Anonymity and unlinkability are commonly accepted features. Untraceability is sometimes used to cover both anonymity and unlinkability.

The reliability of distributed information provides assurance to a receiver that the received information on an event is a true report. Normally, vehicles communicating with each other do not have a strong trust relation. As suggested in the literature, message reliability can be achieved by some threshold method, that is, the receiver only accepts a message that has been confirmed by multiple vehicles (e.g., [2]–[4] and [7]).

The property of revocation means that, if a source is no longer legitimate, it should not be able to send a valid message. There are various methods to achieve this property. One example is to rely on a trusted revocation authority who, for each vehicle, holds a piece of information enabling him to retrieve the vehicle owner's identity from any anonymous message. If a vehicle is no longer legitimate, the authority releases this information, and then, verifiers will reject all messages from that vehicle, as addressed for a target in [4].

Three schemes were proposed in Kounga *et al.* [4], which achieved various levels of security. The first, "basic," and the second, "scalable," solutions address the problems of certificate and key management, whereas the third, "optimized," solution aims to provide the aforementioned four security properties: authentication, privacy (anonymity and unlinkability), reliability, and revocation.

In the remainder of this paper, we will first briefly review the third solution (which we will denote as the *KWL scheme*) and then show that this solution fails to achieve any of its goals. We emphasize, however, that we have only applied our attacks to the KWL scheme (the third solution) and that they do not invalidate the other solutions, which were proposed to address different issues.

II. KWL Scheme

We now give an overview of this scheme. In the scheme, a CA uses a master private key to generate multiple private keys, each of which is given to a tamper-resistant black box associated with a vehicle. A black box then uses its private key to generate multiple short-term certificates for short-term public/private key pairs. This would provide a proof of legitimacy. Unlinkability would be achieved by the constant updates of the short-term certificates—messages broadcast while using one certificate should not be linkable to messages broadcast using another. The details of the scheme are as follows.

The CA holds a secret key K and computes a check value $V = h(g^{AK})$, where h is a one-way hash function, and g is a generator of a group G of order q for some large prime q. Both A and K are large positive integers. It is assumed that the discrete logarithm problem in $G = \langle g \rangle$ is hard, which means that, for any polynomial-time Turing machine, solving this problem is computationally infeasible. The value V and a certificate $Cert\{V\}$, which is signed by the CA, are available to all vehicles. Each vehicle C_k (with index k) is equipped with a tamper-resistant black box BB_k. Other global parameters include m, which is the maximum number of short-term key pairs that can be generated by a black box, and *lifeTime*, which is the validity period of each such key pair. Another hash function f is also available to all black boxes.

At the point of manufacture, the black box BB_k is loaded with the following values:

1) V and $Cert\{V\}$;
2) s_k, which is a secret value specific to BB_k;
3) $P_k = \prod_{j=0}^{m} f^j(s_k)$, where j is an integer, and $f^j(s_k)$ denotes an operation that takes the value s_k as input and runs the function f j times, i.e., $f^j(s_k) = f(f^{j-1}(s_k))$;
4) Q_k, which is a positive integer computed by the CA that satisfies the equation $K = P_k Q_k + r_k$, where r_k is also a positive integer;
5) $g^{r_k} \in G$, where r_k is computed by the CA as above and is only known to the CA;
6) A;
7) global parameters, including g, h, f, m, and *lifeTime*;
8) other global conditions, including *nbSignatures*, which is the minimum number of signed messages reporting on an event that must be received for the report to be considered reliable, and *maxTime*, which is the maximum duration in which these messages must be received.

Note that the CA's secret key K has to be chosen so that $K \gg P_k$ for all P_k.

Note also that the CA stores the value $R_k = g^{Ar_k}$ as a piece of revocation information. When the CA decides that the vehicle C_k is no longer legitimate, the CA can revoke it by publishing this information.

To generate the short-term certificate to be used in the time interval T_i, BB_k chooses a secret random integer a_i such that

$$\begin{aligned} &Aa_i r_k \bmod P_k = 0 \\ &a_i \neq a_{i+n} \quad \text{for} \quad i \in \{0, \ldots, m-1\} \\ &\qquad\qquad\qquad\quad n \in \{1, \ldots, m-i-1\}. \end{aligned}$$

It is not clear from [4] how $Aa_i r_k$ is computed, since BB_k does not know r_k. It could perhaps simply choose $a_i = lP_k/A$ for some random l.

The private key K_i for this time interval is then

$$K_i = Aa_i Q_k \prod_{j=0}^{m-i-1} f^j(s_k)$$

and the corresponding public key is $G_i = g^{K_i}$. The helper value H_i and the value L_i are also computed by BB_k, where

$$\begin{aligned} H_i &= \frac{1}{a_i} \prod_{j=m-i}^{m} f^j(s_k), \\ L_i &= g^{\frac{Aa_i r_k}{P_k} \prod_{j=0}^{m-i-1} f^j(s_k)}. \end{aligned}$$

Finally, BB_k generates a short-term public/private key pair $pub_{T_i}/priv_{T_i}$ and transfers them to C_k along with G_i, H_i, L_i, and $Cert_i$, which is a certificate for pub_{T_i} signed using BB_k's private key K_i.

To broadcast a message msg, C_k signs it with private key $priv_{T_i}$ to get a signature, which is denoted $\{msg\}_{priv_{T_i}}$, and broadcasts the following:

$$\{msg\}_{priv_{T_i}}, Cert_i, G_i, H_i, L_i.$$

For verification, a receiver $C_{k'}$ $(k' \neq k)$ calculates $V^* = (G_i L_i)^{H_i}$ and checks that $h(V^*) = V$. If the equation holds, then $C_{k'}$ uses G_i to check that $Cert_i$ is correctly signed. If the vehicle C_k has been revoked, the verifier can obtain the value R_k from the CA and verify $R_k G_i^{H_i} = V^*$.

The scheme aims to provide four security features.

1) *Unlinkability.* By changing K_i and associated values at frequent intervals, the scheme prevents tracing of vehicles across the time intervals.
2) *Authentication.* A valid signature provides assurance that the message originated from a legitimate source.
3) *Reliability.* By using the tamper-resistant box BB_k, it is guaranteed that each vehicle C_k is only given one valid short-term public/private key pair $pub_{T_i}/priv_{T_i}$ in every time interval and a maximum number m of such short-term key pairs in the lifetime of the secret s_k. This key generation control provides assurance that multiple signatures on one event in the same interval must come from multiple vehicles.
4) *Revocation.* By having the CA as a revocation agency, an illegitimate vehicle C_k can be revoked.

However, in the next section, we will show that none of these goals are achieved.

III. Attacks

We first show that the scheme does not achieve unlinkability. We note that, for any $i \in \{0, \ldots, m-1\}$

$$K_i H_i = A a_i Q_k \prod_{j=0}^{m-i-1} f^j(s_k) \cdot \frac{1}{a_i} \prod_{j=m-i}^{m} f^j(s_k) = A Q_k P_k.$$

Hence, we have $g^{K_i H_i} = g^{K_j H_j}$ for any $i, j \in \{0, \ldots, m-1\}$. Since this is a value specific to BB_k (and C_k), and the values g^{K_i} and H_i are broadcast with every message, an eavesdropper will be able to link the activities of C_k across all certificate updates.

We show next that any adversary who has observed one legitimate message can masquerade as a legitimate black box. Note that verification of the legitimacy of a message is done by computing $V^* = (G_i L_i)^{H_i}$ and checking that $h(V^*) = V$. Hence, any observer of a message can compute V^* from the broadcast information. After obtaining V^*, an adversary simply chooses values u and v and sets $\tilde{K}_i$, $\tilde{G}_i$, $\tilde{H}_i$, and $\tilde{L}_i$ as follows:

$$\begin{aligned} \tilde{K}_i &= uv \\ \tilde{G}_i &= g^{uv} \\ \tilde{H}_i &= \frac{1}{v} \\ \tilde{L}_i &= \left(\frac{V^*}{g^u}\right)^v. \end{aligned}$$

The adversary may then generate a public/private key pair $\widetilde{pub}_{T_i}/\widetilde{priv}_{T_i}$, construct a valid $\widetilde{Cert}_i$ using $\tilde{K}_i$, and send any message msg as

$$\{msg\}_{\widetilde{priv}_{T_i}}, \widetilde{Cert}_i, \tilde{G}_i, \tilde{H}_i, \tilde{L}_i.$$

A receiver would calculate

$$(\tilde{G}_i \tilde{L}_i)^{\tilde{H}_i} = \left(g^{uv}\left(\frac{V^*}{g^u}\right)^v\right)^{\frac{1}{v}} = V^*$$

and accepts the message as legitimate. Hence, the goal of authentication is not achieved.

Note also that the aforementioned "forged" short-term private key $\tilde{K}_i$ and its associated values are indistinguishable from an "authentic" key K_i and its associated values. The adversary can create as many such keys as he wants in any time interval, and the total number of such "valid" keys is not restricted to the value m. As a result, there is no assurance that multiple signatures on one event in the same interval must be created by multiple vehicles. The functionality of the tamper-resistant black box can be bypassed completely. The scheme, therefore, does not hold the property of message reliability.

Obviously, this adversary can survive under the revocation solution of the KWL scheme, since it is not under the CA's control. Any illegitimate source in the CA's revocation list can also escape from being revoked by performing the same trick as this adversary does.

IV. Conclusion

We have shown that the KWL scheme does not achieve the goals of authenticity of a message, privacy of drivers and vehicles, reliability of distributed information, and revocation of illegitimate vehicles.

References

[1] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proc. 4th ACM VANET*, 2007, pp. 19–28.

[2] V. Daza, J. Domingo-Ferrer, F. Sebé, and A. Viejo, "Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 4, pp. 1876–1886, May 2009.

[3] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw.*, 2004, pp. 29–37.

[4] G. Kounga, T. Walter, and S. Lachmund, "Proving reliability of anonymous information in VANETs," *IEEE Trans. Veh. Technol.*, vol. 58, no. 6, pp. 2977–2989, Jul. 2009.

[5] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[6] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: Design and architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[7] M. Raya, A. Aziz, and J.-P. Hubaux, "Efficient secure aggregation in VANETs," in *Proc. 3rd VANET*, 2006, pp. 67–75.

A General Framework for Symbol Error Probability Analysis of Wireless Systems and Its Application in Amplify-and-Forward Multihop Relaying

Golnaz Farhadi and Norman C. Beaulieu, *Fellow, IEEE*

***Abstract*—New exact single-integral expressions for the evaluation of the average error probability of a wireless communication system are derived for a variety of modulation schemes in terms of the moment-generating function (MGF) of the reciprocal of the instantaneous received signal-to-noise ratio (SNR). The expressions obtained form a framework for performance evaluation of wireless communication systems for which the well-known MGF-based performance analysis method cannot be used, that is, systems for which the MGF of the instantaneous received SNR is not known or cannot be derived in closed-form. Using the framework obtained, the error probability performance in general fading of an amplify-and-forward (AF) multihop relaying system with both variable-gain and fixed-gain relays is then evaluated. In particular, a new expression for the MGF of the reciprocal of the instantaneous received SNR of an AF multihop system with fixed-gain relays is derived. Numerical examples show precise agreement between simulation results and theoretical results.**

***Index Terms*—Amplify-and-forward (AF) relaying, error probability, moment-generating function (MGF), multihop transmission.**

I. Introduction

Multihop transmission has emerged as a promising technique for extending coverage, enhancing connectivity, and saving transmitter power in wireless communications networks. In a multihop transmission system, a source communicates with the destination through several intermediate terminals called relays.

The theoretical evaluation of the average error probability of a wireless communication system in fading is generally done using

Manuscript received June 11, 2009; revised October 9, 2009. First published December 4, 2009; current version published March 19, 2010. This work was supported in part by an Alberta Ingenuity Studentship, by an Alberta Informatics Circle of Research Excellence (*i*CORE) Scholarship, and by an *i*CORE Research Chair Establishment Grant. The review of this paper was coordinated by Prof. Y. Su.

The authors are with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB T6G 2V4, Canada (e-mail: gfarhadi@ece.ualberta.ca; beaulieu@ece.ualberta.ca).

Digital Object Identifier 10.1109/TVT.2009.2037642